034

Laszlo Csirmaz
Central European University

How Secure Cryptographic Protocols Are?

Breaking the MD5 hash (digest) algorithm was the biggest sensation of the last year, at least in cryptopgrahic circles. The MD5 algorithm is used widely, both by MS Word and MS Excel among others, for ensuring integrity of a document. The properties of a safe digest algorithm ensure that changing a document in any way changes its digest as well. Using the above mentioned crytographic result it is by no means hard to create two different documents with identical hash values.

Can we trust cryptographic algorithms after all? What happens if all used cryto algorithms are broken? Isn't it possible that all hackers of the word could use troyan horses to steal all computers and force them to recover secret keys? What would happen when quantum computers will be available at the corner store, and using them all RSA keys would be recovered in minutes?

Cryptopgraphers around the world are not worried at all. Dozens of algorithms based on extremely diverse principles are available right now for all basic tasks: for hash functions, for symmetric and asymmetric encryption. Any of these algorithms may turn out to be too weak. But in any case, there will always be a new one around to be used.